

Remarks

A. Background

Claims 1-24 are pending. The Office Action asserts a 35 U.S.C. § 102(e) rejection against claims 1-24 as being anticipated by Gruse et al. (*Gruse*) U.S. Patent No. 6,398,245. In light of the following remarks, Applicants respectfully request reconsideration of those claims.

B. Patentability of the Claims

In order to establish a *prima facie* case of anticipation, the basic criteria is that the “each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference.” (MPEP § 2131).

The Applicants respectfully submit that the 35 U.S.C. § 102(e) rejection is improper for at least the following reason: *Gruse* does not teach or suggest “determining which one of a plurality of data rights management architectures corresponds to said first data rights management architecture” as recited in claim 1 of the pending patent application.

Independent claims 16, 17, 18, 21, 22, and 24 recite similar limitations. For example, claim 16 recites “a permit system interfaced to said order management system that determines which one of plurality of data rights management architectures corresponds to said first data rights management architecture, that generates a permit based on said determined one of said plurality of data rights management architectures, and that provides said permit in response to said request to provide access rights to protected content;” claim 17 recites a “means for determining which one of a plurality of data rights management architectures corresponds to a particular permit request;” claim 18 recites “determining which one of a plurality of data rights management architectures corresponds to said first data rights management architecture;” claim 21 recites “determining which one of a plurality of permit classes was used to protect a piece of protected content;” claim 22 recites “receiving a request from a packager for a first permit class to protect a piece of content, said first permit class associated with a first data rights management architecture;” and claim 24 recites “receiving a request from a sponsor for a first permit class, said first permit class associated with a first data rights management architecture . . . [and] receiving a request for a

second permit class, said second permit class associated with a second data rights management architecture.” Therefore, for this and the following reasons, claims 1, 16, 17, 18, 21, 22, and 24 are not anticipated by *Gruse*.

The Office Action cites the “Electronic Digital Content Store(s) Embodiment” portion of *Gruse* as anticipating claim 1. Applicants submit that the Office Action fails to appreciate key differences between *Gruse* and the claimed invention. For example, *Gruse* does not determine which one of a plurality of data rights management architectures corresponds to a first data rights management architecture. Instead, *Gruse* describes a digital rights management (DRM) architecture that allows web retailers to distribute digital content (See *Gruse*, col. 11, lines 56-60, which states, “the Secure Digital Content Electronic Distribution System (System) is an open architecture with published specifications and interfaces to facilitate broad implementation and acceptance of the System in the market place. . . .”). As noted in the pending application’s specification, there are numerous incompatible DRM architectures for protecting content throughout the industry, e.g., Intertrust, Microsoft, Adobe Systems, Preview Systems, Xerox Corporation, and IBM all provide DRM architecture solutions (see page 3, lines 23-26). *Gruse* describes one of these systems.

For example, once users have properly authenticated to the *Gruse* system using digital certificates, they can download digital content. Downloading digital content includes a key management system in which “digital content data encrypted with a first encrypting key is decrypted using a first decrypting key, and re-encrypted using a second encrypting key. A second decrypting key is encrypted using a third encrypting key to produce an encrypted second decrypting key.” (*Gruse*, col. 6, lines 28-33). *Gruse* further describes a digital content player that “includes a decrypter that decrypts digital content data, which was encrypted with a first encrypting key, using a first decrypting key so as to produce the content data. An encrypter re-encrypts the content data using a second encrypting key and encrypts a second decrypting key using a third encrypting key. In one preferred content player, a receiver receives an encrypted first decrypting key that was encrypted using a fourth encrypting key, and the decrypter decrypts the encrypted first decrypting key using a fourth decrypting key to reproduce the first decrypting key.” (*Gruse*, col. 6, lines 47-56). Basically, *Gruse* provides an encryption/decryption key architecture to securely distribute digital content to end users. In other words, *Gruse* describes the type of architecture claim 1 “determin[es] . . . corresponds to said first data rights

management architecture.” In other words, *Gruse* is its own DRM architecture and does no comparison to “determine[e] which one of a plurality of data rights management architectures corresponds to said first data rights management architecture” as recited in claim 1.

Within the context of the Electronic Digital Content Store(s) Embodiment cited in the Office Action, *Gruse* requests digital certificates conforming to specific guidelines, e.g., a digital certificate “includes a version number, a unique serial number, the signing algorithm, the name of the issuer . . . , a range of dates for which the certificate is considered to be valid, the name of the Electronic Digital Content Store(s), the public key of the Electronic Digital Content Store(s), and a has code of all of the other information signed using the private key of the Clearinghouse(s).” (*Gruse*, col. 46, 31-42). Once a digital certificate has been created and received in the *Gruse* architecture, Electronic Digital Content Store(s) “can begin offering content that can be purchased by End Users.” The digital certificate allows “End-user Device(s) to verify that the Electronic Digital Content Store(s) is a valid distributor of Content on the secure Digital Content Electronic Distribution System.” (*Gruse*, col. 46, lines 42-53). The portion of the prior art reference the Office Action cites against claim 1 relates to the process of authenticating distributors in a digital retailer hierarchy. Basically, the digital certificates authenticate the identities of their subject, but do nothing more.

The pending application, on the other hand, states, “[t]o access protected content within containers, consumers must acquire certain rights. Access rights to the content may be acquired from the content provider, content packager or web retailer. According to the present invention access rights are provided through the use of ‘permits.’ Permits are digital devices that allow consumers to access protected content.” (Specification, page 10, line 25 – page 11, line 1). In other words, the digital certificates are not a “permit” as recited in claim 1 nor do they help “determin[e] which one of a plurality of data rights management architectures corresponds to said first data rights management architecture.” They merely authenticate users to the system. Thus, the portions of *Gruse* describing digital certificates cited by the Office Action are improperly associated with the “permit” recited in claim 1.

Moreover, the Office Action cites to those parts of *Gruse* that describe tools for implementing the Electronic Digital Content Store(s). (Office Action, page 3). Applicants respectfully note that the tools and toolkit described by *Gruse* “are designed to allow flexibility in how the Electronic Digital Content Store(s) wishes to integrate sale of downloadable

electronic Content into its service" and do not describe "determining which one of a plurality of data rights management architectures corresponds to said first data rights management architecture" as recited in claim 1. (See *Gruse*, col. 74, lines 28-30). For at least these reasons, Applicants respectfully submit claim 1 is in condition for allowance and earnestly seek such action.

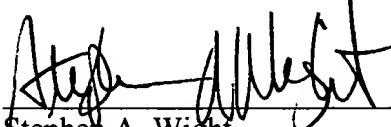
Claims 2-15 depend from claim 1. Because dependent claims include the limitations of the claims from which they depend, Applicants submit that claims 2-15 are also in condition for allowance. For similar reasons, Applicants submit that independent claims 16, 17, 18, 21, 22, 24, and their dependent claims are also in condition for allowance.

C. Conclusion

For at least the foregoing reasons, Applicants submit that the rejection under 35 U.S.C. § 102(e) has been overcome. Therefore, claims 1-24 are in condition for allowance and such action is earnestly solicited. The Examiner is respectfully requested to contact the undersigned by telephone if it is believed that such contact would further the examination of the present application.

Respectfully submitted,

KLARQUIST SPARKMAN, LLP

By 
Stephen A. Wight
Registration No. 37,759

One World Trade Center, Suite 1600
121 S.W. Salmon Street
Portland, Oregon 97204
Telephone: (503) 226-7391 / Facsimile: (503) 228-9446